UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/822,788	04/13/2004	Alan Azralon	CSC-001	3255

51414 7590 11/28/2007

GOODWIN PROCTER LLP
PATENT ADMINISTRATOR
EXCHANGE PLACE
BOSTON, MA 02109-2881

EXAMINER	
GRAHAM, PAUL J	
ART UNIT	**PAPER NUMBER**
2623	

MAIL DATE	DELIVERY MODE
11/28/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/822,788	AZRALON ET AL.	
	Examiner	Art Unit	
	Paul J. Graham	2623	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *13 April 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-32* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-32* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *13 April 2004* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Information Disclosure Statement

Drawings

1. New corrected drawings in compliance with 37 CFR 1.121(d) are required in this application because fig. 1 drawings are lacking a text label for each enumerated item shown. Applicant is advised to employ the services of a competent patent draftsperson outside the Office, as the U.S. Patent and Trademark Office no longer prepares new drawings. The corrected drawings are required in reply to the Office action to avoid abandonment of the application. The requirement for corrected drawings will not be held in abeyance.

Specification

2. The specification is objected to because of the following informalities:

3. In the incorporation by reference, the version number of the Enhanced Content Specification is omitted. Appropriate correction is required.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 1, 2, 4-6, 8, 9, 10, 12, 13, 15-18, 20-22, 24, 25, 27 are rejected under 35 U.S.C. 103(a) as being unpatentable over Leak et al. (US 7174562 B1) in view of Sprunk (US 2006/0053439 A1) in further view of Blackletter et al. (US 2005/0172331 A1).

As to claim 1, Leak discloses a method for controlling access to an enhancement within a trigger, comprising (see Leak, col. 3, l. 30-col. 4, l. 62):

determining whether a received signal includes the trigger (see Leak, col. 1, ll. 44-51, determination is made based on display of offering icon);

Leak does not teach encrypting a portion of the trigger; however, Sprunk, who discloses an network object and resource security system, does teach that a video object (such as the collection of data in a trigger, see Sprunk, [0039]) can be transmitted in encrypted form (see Sprunk, [0050]).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the method of Leak with the system of Sprunk to allow for the encryption and greater security over a large network such as the internet (and subsequent decryption) of a video stream object like a trigger (see Sprunk, [0050]). After receipt, the object will be decrypted (see Sprunk, fig. 3);

Leak nor Sprunk teach determining to display to the user; however, Blackletter, who discloses communicating scripts in a video signal, does teach this (see Blackletter, [0052 & 0065]); when a predetermined criteria like the trigger matches the URL (see Blackletter, fig. 6) then the script is executed to allow a webpage to be displayed to a user.

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the system of Blackletter with the system of Leak and Sprunk in order to make use of the trigger as a decision rule (see Blackletter, [0015]).

As to claim 2, Leak, Sprunk and Blackletter (as combined in claim 1) disclose the method of claim 1, further comprising preventing display of the enhancement to the user when the decrypted portion does not meet the predetermined criteria (see Blackletter, fig. 6, when criteria is not met (trigger not equal URL) the script is disregarded, and the display is prevented).

As to claim 4, Leak, Sprunk and Blackletter (as combined in claim 1) disclose method of claim 3, wherein encrypting a portion of the trigger further comprises inserting the encrypted uniform resource locator into a script portion of the trigger (see Blackletter, [0037-0038], the URL is embedded in the script newWeather).

As to claim 5, Leak, Sprunk and Blackletter (as combined in claim 1) disclose the method of claim 1, wherein determining whether the decrypted portion meets predetermined criteria comprises comparing the decrypted portion of the trigger to a uniform resource locator portion of the trigger (see Blackletter, fig. 6).

As to claim 6, Leak, Sprunk and Blackletter (as combined in claim 1) disclose the method of claim 1, wherein encrypting a portion of the trigger comprises inserting an activation date and/or a deactivation date (see Leak, fig. 2, "expires")

Leak does not explicitly teach that the expiration date is inserted into the encrypted portion of the trigger; however, official notice is taken that given the combination of Leak and Sprunk for security purposes it is well known in the art that something (e.g., the expiration date of the trigger) that is sensitive to security matters could be placed in the encrypted portion of the trigger.

As to claim 8, Leak, Sprunk and Blackletter (as combined in claim 1) disclose the method of claim 6, wherein determining whether the decrypted portion meets predetermined criteria comprises comparing whether the deactivation date is subsequent to a current date (see Leak, fig. 2 and col. 4, ll. 48-63, a current date is inherently set by the operator who provided the time stamp.

As to claim 9, Leak discloses a method of controlling access to an enhancement within a trigger, comprising (see Leak, col. 3, l. 30-col. 4, l. 62):

determining whether a signal includes the trigger (see Leak, col. 1, ll. 44-51, determination is made based on display of offering icon);

receiving a portion of a trigger (see Leak, fig. 1);

Leak does not teach encrypting a portion of the trigger; however, Sprunk, who discloses an network object and resource security system, does teach that a video object (such as the collection of data in a trigger, see Sprunk, [0039]) can be transmitted (or included with trigger to be sent) in encrypted form (see Sprunk, [0050]).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the method of Leak with the system of Sprunk to allow for the encryption and greater security over a large network such as the internet (and subsequent decryption) of a video stream object like a trigger (see Sprunk, [0050]).

After receipt, the object will be decrypted (see Sprunk, fig. 3);

Leak nor Sprunk teach determining to display to the user; however, Blackletter, who discloses communicating scripts in a video signal, does teach this (see Blackletter, [0052 & 0065]); when a predetermined criteria like the trigger matches the URL (see Blackletter, fig. 6) then the script is executed to allow a webpage to be displayed to a user.

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the system of Blackletter with the system of Leak and Sprunk in order to make use of the trigger as a decision rule (see Blackletter, [0015]).

As to claims 10, 12, 13, and 15, they are analyzed similarly to claims 2, 4, 5, and 8, respectively (see above).

As to claim 16, Leak discloses an apparatus (see fig. 4, receiver) to control access to an enhancement within a trigger, comprising (see Leak, col. 3, l. 30-col. 4, l. 62):

Leak does not explicitly teach the functional components of a receiver (STB); however, Blackletter, who discloses communicating scripts in a video signal, does teach this (see Blackletter, fig. 3).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the apparatus system of Leak with the apparatus of Blackletter, to give some insight into the functional componentry of a set-top box for use in interactive TV situation (see Blackletter, [0014-0015]).

Blackletter depicts a processor (see Blackletter, fig. 3); a memory to store instructions to be executed by the processor (see Blackletter, fig. 3, RAM/ROM), the instructions including instructions to (see Blackletter, [0016]):

determining whether a received signal includes the trigger (see Blackletter, [0015]);

and if the decrypted portion meets predetermined criteria, allowing display of the enhancement to a user (see Blackletter, fig. 6) then the script is executed to allow a webpage to be displayed to a user);

Leak or Blackletter do not explicitly teach decrypting a portion of the trigger; however, Sprunk, who discloses the encryption and decryption of video objects does teach decrypting a portion of the trigger (see Sprunk, fig. 3, decrypt the object).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the Apparatus of Leak and Blackletter with the system of Sprunk in order to allow for the decryption of a data object such as that found in a trigger in a signal (see Sprunk [0031]).

As to claims 17, 18, and 20, they are analyzed similar to claims 2, 5, and 8, respectively (see above).

As to claim 21, Leak discloses a system to control access to an enhancement within a trigger, comprising (see Leak, col. 3, l. 30-col. 4, l. 62):

a second computing unit to receive a signal (see Leak, fig. 1, receiving units),

determine whether the signal includes the trigger (see Leak, col. 1, ll. 44-51, determination is made based on display of offering icon),

Leak does teach a TV broadcasting transmission unit; Leak does not explicitly teach a first unit to receive a portion of the trigger (say a URL from the internet); however, Sprunk does teach this (see Sprunk, fig. 1, the headend).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the system of Leak with the system of Sprunk to allow for a 1st receiving unit to receive the trigger from a content source (see Sprunk [0031]).

a first computing unit to receive a portion of a trigger (see Leak, fig. 1, receiving units),

encrypt the portion of the trigger (see Sprunk, [0039], a video object, such as data in a trigger, can be encrypted),

and send the encrypted portion to be included with the trigger (see Sprunk [0050] sent with trigger transmitted in an encrypted form);

decrypt the encrypted portion of the trigger (see Sprunk, fig. 3, decrypt the object),

Leak nor Sprunk teach determining to display to the user; however, Blackletter, who discloses communicating scripts in a video signal, does teach this (see Blackletter, [0052 & 0065]); when a predetermined criteria like the trigger matches the URL (see Blackletter, fig. 6) then the script is executed to allow a webpage to be displayed to a user.

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the system of Blackletter with the system of Leak and Sprunk in order to make use of the trigger as a decision rule (see Blackletter, [0015]).

As to claims 22, 24, 25, and 27 they are analyzed similar to claims 2, 4, 5, and 8, respectively (see above).

6. Claims 3, 11, 23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Leak et al. (US 7174562 B1) in view of Sprunk (US 2006/0053439 A1) in view of Blackletter et al. (US 2005/0172331 A1) in further view of Hon et al. (US 2007/0255960 A1).

As to claim 3 Leak, Sprunk and Blackletter (as combined in claim 1) disclose the method of claim 1, wherein encrypting a portion of the trigger

Leak, Sprunk or Blackletter do not teach encrypting a uniform resource locator; however, Hon, who discloses a system for validation in a network, does teach this (see Hon, [0011]).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the system of Leak, Sprunk and Blackletter with the system of Hon to ensure that a public key may be coming from its legitimate owner over an network such as the internet (see Hon, [0011]).

As to claims 11 and 23, they are analyzed similar to claim 3 (see above).

7. Claims 7, 14, 19, and 26 are rejected under 35 U.S.C. 103(a) as being unpatentable over Leak et al. (US 7174562 B1) in view of Sprunk (US 2006/0053439 A1) in view of Blackletter et al. (US 2005/0172331 A1) in further view of Knight et al. (US 2006/0242327 A1).

As to claim 7, Leak, Sprunk and Blackletter (as combined in claim 1) disclose the method of claim 6,

Leak, Sprunk or Blackletter do not teach comparing the activation date (or time) with a current time (or date); however, Knight, who discloses a system for data synchronization does teach comparing an activation time with a current time (see Knight, [0048], the trigger is initiated when the activation time (or sync time) is before the current time, a predetermined criteria, see fig. 5).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the system of Leak, Sprunk and Blackletter with the system of Knight in order to trigger the initiation of activity according to some decision rule (see Knight, [0009]).

As to claims 14, 19, and 26, they are analyzed similar to claim 7 (see above).

8. Claims 28 and 30 are rejected under 35 U.S.C. 103(a) as being unpatentable over Leak et al. (US 7174562 B1) in view of Sprunk (US 2006/0053439 A1) in view of Blackletter et al. (US 2005/0172331 A1) in further view of Steenkamp et al. (US 2004/0168184 A1).

As to claim 28, Leak discloses a method for controlling access to an enhancement within a trigger, comprising (see Leak, col. 3, l. 30-col. 4, l. 62):

determining whether a received signal includes the trigger (see Leak, col. 1, ll. 44-51, determination is made based on display of offering icon);

Leak does not teach encrypting a portion of the trigger; however, Sprunk, who discloses a network object and resource security system, does teach that a video object

(such as the collection of data in a trigger, see Sprunk, [0039]) can be transmitted in encrypted form (see Sprunk, [0050]).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the method of Leak with the system of Sprunk to allow for the encryption and greater security over a large network such as the internet (and subsequent decryption) of a video stream object like a trigger (see Sprunk, [0050]).

After receipt, the object will be decrypted (see Sprunk, fig. 3);

Leak nor Sprunk teach determining to display to the user; however, Blackletter, who discloses communicating scripts in a video signal, does teach this (see Blackletter, [0052 & 0065]); when a predetermined criteria like the trigger matches the URL (see Blackletter, fig. 6) then the script is executed to allow a webpage to be displayed to a user.

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the system of Blackletter with the system of Leak and Sprunk in order to make use of the trigger as a decision rule (see Blackletter, [0015]).

Leak or Sprunk or Blackletter do not explicitly teach a medium with executable instructions; however, Steenkamp, who discloses a multi-content provider interface does teach a machine-readable medium (see fig. 22) having stored thereon a plurality of executable instructions, the plurality of instructions comprising instructions to (see Steenkamp, [0489]).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the system of Leak, Sprunk, and Blackletter with the system of Steenkamp so that the method of manipulating a video stream may be automated with a machine-readable medium (see Steenkamp, [0489]).

Leak or Sprunk or Blackletter do not explicitly teach a head-end type with componentry for upstream operations; however, Steenkamp, who discloses a multi-provider interface, does teach this.

Steenkamp shows a processor (see Steenkamp, fig. 22); a memory to store instructions to be executed by the processor (see Steenkamp, fig. 22), the instructions including instructions to:

receive at least a portion of the trigger (see Steenkamp, fig. 20, receive comm. from content distributor); encrypt the portion of the trigger (see Steenkamp, fig. 5, cryptographic operation); and send the encrypted portion of the trigger to be included in a signal including the trigger (see Steenkamp, fig. 22, signal generation).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the apparatus of Leak with the apparatus and system of Steenkamp in order to explicitly execute the upstream operations of a headend unit (see Steenkamp, [0489]).

As to claim 30, it is analyzed similar to claim 6 (see above).

9. Claim 29 is rejected under 35 U.S.C. 103(a) as being unpatentable over Leak et al. (US 7174562 B1) in view of Sprunk (US 2006/0053439 A1) in view of Blackletter et al. (US 2005/0172331 A1) in view of Steenkamp et al. (US 2004/0168184 A1) in further view of Hon et al. (US 2007/0255960 A1).

As to claim 29, Leak discloses a method for controlling access to an enhancement within a trigger, comprising (see Leak, col. 3, l. 30-col. 4, l. 62):

determining whether a received signal includes the trigger (see Leak, col. 1, ll. 44-51, determination is made based on display of offering icon);

Leak does not teach encrypting a portion of the trigger; however, Sprunk, who discloses a network object and resource security system, does teach that a video object (such as the collection of data in a trigger, see Sprunk, [0039]) can be transmitted in encrypted form (see Sprunk, [0050]).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the method of Leak with the system of Sprunk to allow for the encryption and greater security over a large network such as the internet (and subsequent decryption) of a video stream object like a trigger (see Sprunk, [0050]).

After receipt, the object will be decrypted (see Sprunk, fig. 3);

Leak nor Sprunk teach determining to display to the user; however, Blackletter, who discloses communicating scripts in a video signal, does teach this (see Blackletter, [0052 & 0065]); when a predetermined criteria like the trigger matches the URL (see Blackletter, fig. 6) then the script is executed to allow a webpage to be displayed to a user.

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the system of Blackletter with the system of Leak and Sprunk in order to make use of the trigger as a decision rule (see Blackletter, [0015]).

Leak or Sprunk, Blackletter or Steenkamp do not explicitly teach encrypting a uniform resource locator; however, Hon, who discloses a system for validation in a network, does teach this (see Hon, [0011]).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the system of Leak, Sprunk and Blackletter with

the system of Hon to ensure that a public key may be coming from its legitimate owner over an network such as the internet (see Hon, [0011]).

10. Claims 31 and 32 are rejected under 35 U.S.C. 103(a) as being unpatentable over Leak et al. (US 7174562 B1) in view of Sprunk (US 2006/0053439 A1) in view of Blackletter et al. (US 2005/0172331 A1) in further view of Steenkamp et al. (US 2004/0168184 A1).

As to claim 31, Leak discloses a method for controlling access to an enhancement within a trigger, comprising (see Leak, col. 3, l. 30-col. 4, l. 62):

determining whether a received signal includes the trigger (see Leak, col. 1, ll. 44-51, determination is made based on display of offering icon);

Leak does not teach encrypting a portion of the trigger; however, Sprunk, who discloses a network object and resource security system, does teach that a video object (such as the collection of data in a trigger, see Sprunk, [0039]) can be transmitted in encrypted form (see Sprunk, [0050]).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the method of Leak with the system of Sprunk to allow for the encryption and greater security over a large network such as the internet (and subsequent decryption) of a video stream object like a trigger (see Sprunk, [0050]).

After receipt, the object will be decrypted (see Sprunk, fig. 3);

Leak nor Sprunk teach determining to display to the user; however, Blackletter, who discloses communicating scripts in a video signal, does teach this (see Blackletter, [0052 & 0065]); when a predetermined criteria like the trigger matches the URL (see

Blackletter, fig. 6) then the script is executed to allow a webpage to be displayed to a user.

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the system of Blackletter with the system of Leak and Sprunk in order to make use of the trigger as a decision rule (see Blackletter, [0015]).

Leak or Sprunk or Blackletter do not explicitly teach a medium with executable instructions; however, Steenkamp, who discloses a multi-content provider interface does teach a machine-readable medium (see fig. 22) having stored thereon a plurality of executable instructions, the plurality of instructions comprising instructions to (see Steenkamp, [0489]).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the system of Leak, Sprunk, and Blackletter with the system of Steenkamp so that the method of manipulating a video stream may be automated with a machine-readable medium (see Steenkamp, [0489]).

As to claim 32, Leak discloses a method for controlling access to an enhancement within a trigger, comprising (see Leak, col. 3, l. 30-col. 4, l. 62):

determining whether a received signal includes the trigger (see Leak, col. 1, ll. 44-51, determination is made based on display of offering icon);

Leak does not teach encrypting a portion of the trigger; however, Sprunk, who discloses a network object and resource security system, does teach that a video object (such as the collection of data in a trigger, see Sprunk, [0039]) can be transmitted in encrypted form (see Sprunk, [0050]).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the method of Leak with the system of Sprunk to allow for the encryption and greater security over a large network such as the internet (and subsequent decryption) of a video stream object like a trigger (see Sprunk, [0050]). After receipt, the object will be decrypted (see Sprunk, fig. 3);

Leak nor Sprunk teach determining to display to the user; however, Blackletter, who discloses communicating scripts in a video signal, does teach this (see Blackletter, [0052 & 0065]); when a predetermined criteria like the trigger matches the URL (see Blackletter, fig. 6) then the script is executed to allow a webpage to be displayed to a user.

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the system of Blackletter with the system of Leak and Sprunk in order to make use of the trigger as a decision rule (see Blackletter, [0015]).

Leak or Sprunk or Blackletter do not explicitly teach a medium with executable instructions; however, Steenkamp, who discloses a multi-content provider interface does teach a machine-readable medium (see fig. 22) having stored thereon a plurality of executable instructions, the plurality of instructions comprising instructions to (see Steenkamp, [0489]).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the system of Leak, Sprunk, and Blackletter with the system of Steenkamp so that the method of manipulating a video stream may be automated with a machine-readable medium (see Steenkamp, [0489]).

Inquiries

11. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Paul J. Graham whose telephone number is 571-270-1705. The examiner can normally be reached on Monday-Friday 8:00a-5:00p EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Vivek Srivastava can be reached on 571-272-7304. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

ANDREW Y. KOENIG
PRIMARY PATENT EXAMINER

pjg
11/23/07